AFRL-RI-RS-TM-2007-14
Final Technical Memorandum
October 2007

MONITORING TOOLS FOR DOMAIN NAME SYSTEM (DNS) SECURITY DEPLOYMENT

Colorado State University

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

NOTICE AND SIGNATURE PAGE

AFRL-RI-RS-TM-2007-14 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/	/s/
THOMAS PARISI Work Unit Manager	WARREN H. DEBANY, Jr. Technical Advisor, Information Grid Division Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
OCT 2007

2. REPORT TYPE
Final

3. DATES COVERED *(From - To)*
Mar 05 – Apr 07

4. TITLE AND SUBTITLE

MONITORING TOOLS FOR DOMAIN NAME SYSTEM (DNS) SECURITY DEPLOYMENT

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA8750-02-2-0205

5c. PROGRAM ELEMENT NUMBER
G52108

6. AUTHOR(S)

Daniel F. Massey

5d. PROJECT NUMBER
DHSA

5e. TASK NUMBER
CS

5f. WORK UNIT NUMBER
UC

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colorado State University
601 S. Howes St.
Fort Collins CO 80523-0001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

AFRL/RIGA
525 Brooks Rd
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TM-2007-14

12. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED. PA# WPAFB 07-0035

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The Domain Name System (DNS) converts names such as www.afrl.mil into IP addresses that can be used for communication. It is an essential part of almost every Internet application, but lacks authentication mechanisms. The DNS Security Extensions address this problem and add origin authentication into the system. Deployment of the security extensions is now beginning and this project monitors that early deployment. The project provides real-time deployment tracking and identifies several operational challenges and barriers that must be overcome for this system to succeed.

15. SUBJECT TERMS
Security monitoring, Domain Name System

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Thomas Parisi
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (*Include area code)*
U	U	U	UL	13	N/A

Monitoring Tools for DNS Security Deployment

Final Report

Project Objectives

The project consisted of 5 primary tasks:

Task 1: Deployment of Secure Zones

We have deployed secure zones, expand the secondary servers for these zones, and link our zones to existing DNSSEC testbeds.

Task 2: Level 1 Monitoring

We have developed a monitoring toolset that can assess whether DNS zones are currently able to support DNSSEC. We are using this toolset to determine which zones are currently able to deploy DNSSEC. The software called SecSpider is working and is currently deployed.

Task 3: Level 2 Monitoring

We have developed DNSSEC zone correctness monitoring and verification tools as part of the SecSpider package. We are using this toolset to monitor the state of DNSSEC deployment at our zones and zones from other sites. The software is deployed.

Task 4: Level 3 Monitoring

We have developed DNSSEC inter-zone coordination monitoring and verification tools. We are using this SecSpider toolset to monitor the state of DNSSEC deployment at our zones and islands of security (regions of DNSSEC deployment) from other sites. The software is deployed.

Task 5: Analysis, Reporting, and Software Release

As data was collected throughout the project, the results illustrate DNS issues and resulted in discussions with both zone operators and vendors. A full report on the findings is discussed in this report.

Technical Results

Summary of Main Results:

- Following task 1, the project established the infrastructure and skill set to deploy and operate secure zones at both Colorado State University and UCLA. This task is complete. During the project, Colorado State University established a partnership with Secure64. The Secure64 product incorporates design recommendations learned from the project and we now use the Secure64 box to manage our zone. Secure64 is marketing the product.
- Following task 2, the project has produced a SecSpider toolset that can assess whether zones can support DNSSEC. This task is complete and the software is deployed and continues to collect data after the project end. The SecSpider website is available at http://zinc.cs.ucla.edu/secspider/ and has been announced on various DNSSEC mailing lists. An article on SecSpider appeared in the DNSSEC Newsletter and our results were presented at a DNS workshop.
- Following task 3, the project has added DNSSEC monitoring and verification for secure zones. This task is complete and the SecSpider toolset is deployed and collecting data. Several zones have been submitted to the monitoring tool and other zones have been added and/or discovered by the project

team. At the project conclusion, we are monitoring over 1860 zones and have more detailed monitoring for 859 DNSSEC deployed zones.

- Following task 4, the SecSpider toolset monitors the boundaries between zones. This task is complete and tracks the correctness and evolution of islands of DNS security. Data is being collected and logged by the monitoring software. The results so far show a very small number of zones form authentication chains with their parents and this trend is a concern. We recommend automated software for doing this and have presented our designs in various forums. The Secure64 company is considering adopting our recommendations in their next product release.
- Work on task 5 has identified some issues. One challenge is that all servers must deploy DNSSEC, a challenge for zones such as Colorado State University that mix windows and unix boxes. Our measurements show that increasing the TTL on NS, DS, and DNSKEY RRs can dramatically reduce the vulnerability to DDoS attacks; while not an initial planned direction, this observation followed from our monitoring results. and data from task 4 monitoring has led us to recommend a new best practice of setting very long time to live (TTL) values for NS records. This work was submitted as an Internet draft and progress on the draft continues. Our monitoring tool has been used to identify and correct errors in zones and the data provides some interesting insights into how DNSSEC is being deployed.

1. Task 1: Deployment of Secure Zones

A major objective of this project is to monitor the successes and identify the limitations in deploying DNS security. As an essential first step, the project teams at Colorado State University and UCLA need to act as both monitors (the primary objective) and DNSSEC operators (so we can better understand what we are monitoring, test theories, and so forth). Graduate and undergraduate students at both universities have been working on deploying and operating secure zones.

We have created zones netsec.cs.colostate.edu and netsec.cs.ucla.edu at both Colorado State University and UCLA (respectively). Both zones are operational and run variations of DNSSEC, depending on the type of testing needed for our toolset development. The Colorado State University zone is also used by the network security group and as the primary DNS infrastructure for desktop host machines, project web server, and so forth. Below each zone, there are several descendant zones so that each site can configure DNSSEC between zones. We have also produced guides for deploying DNSSEC so future project members can easily gain these initial skills.

The graduate course on network security at Colorado State University required all students to create zones under the netsec.cs.colostate.edu island of security and secure these zones. Our results show the need for better tools that produce this data automatically. A local security company, Secure64, has hired one of the graduate students who was working on this project. All of our guidelines and results are public. Based partly on these guidelines, the Secure64 company has produced a secure and reliable DNS server. We now use this product to manage our zone and the company is marketing the product widely. This task is complete and with the adoption of recommendations by a major vendor we view this as a success.

2. Task 2: Level 1 Monitoring

Using our current DNS monitoring system as a basis, we have built the SecSpider monitoring tool. This tool monitors for zones for ability to deploy DNSSEC, provides a web interface to the data, allows any Internet user to submit a zone for monitoring, and then provides continuous monitoring of that zone.

In testing for the ability to deploy DNSSEC, it is important to note that different versions of DNS servers support different versions of DNSSEC. Testing directly for DNSSEC by querying for DNSSEC records works for zones which have deployed DNSSEC, but fails to provide definitive information for zones that are capable of deploying but have to turn on DNSSEC. A more realistic and achievable approach is to test for the required EDNS0 support and the sufficient buffer size. SecSpider performs these checks and logs the results.

It is not sufficient to simply check a single server. For example, our experience with the campus administration in task 1 shows that zones may operate a number a name servers some of which are DNSSEC capable and others are not. SecSpider tracks the ENDS0 support at all name servers for a zone.

Finally, SecSpider works as a long term monitoring system where a zone's status is continually refreshed. This task is generally complete and has a robust web based user interface at

http://secpsider.cs.ucla.edu/

The website provides various levels of monitoring as discussed in the tasks below.

Although the project has concluded, SecSpider continues to monitor zones and provide public data. We have received a great deal of feedback from the site by DNS operators and some vendors. We plan to continue the site as resources permit and have submitted follow-on projects to add more distributed monitoring to the website.

3. Task 3: Level 2 Monitoring

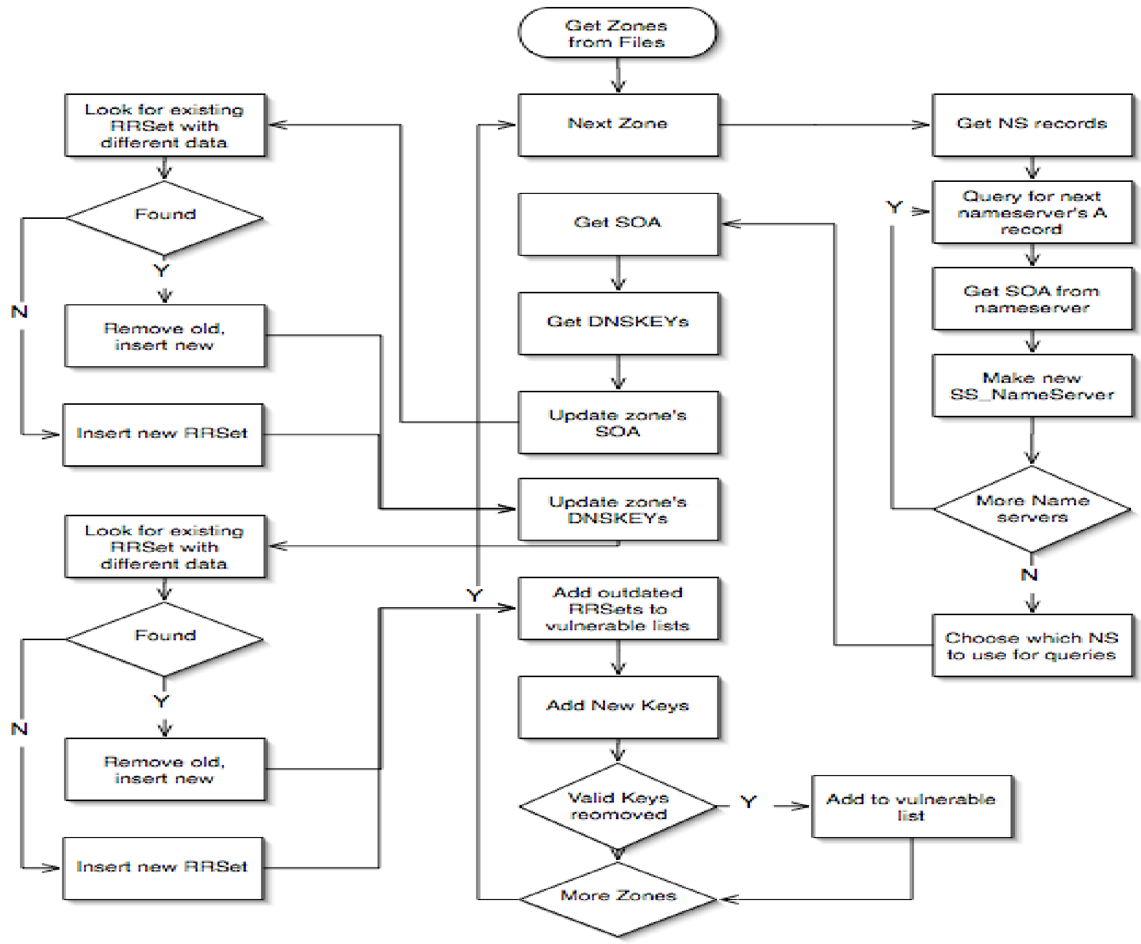
Once a zone has been submitted to the monitoring system, SecSpider evaluates the zone to determine its DNSSEC status and its correctness if DNSSEC is deployed. The zones are then periodically reached from the perspective of each authoritative server for that zone. The process works as follows:

Given a zone name, the SecSpider tool uses standard DNS queries to get the NS (name sever) records for the zone. It then separately queries for the corresponding A (IP address) records for the zones. For completeness and to verify the correctness of each name server, the Sec Spider also retrieves the SOA (start of authority, a mandatory bookkeeping record). These records are stored in a database described later and used for periodic queries for the zones status.

The SecSpider tool then determines the EDNSO (indicator of DNSSEC potential as discussed above) for each server and attempts to retrieve DNSKEYs (required for any zone that deploys DNSSEC). During periodic queries, SecSpider retrieves the SOA and uses the SOA serial number to determine if the zone has changed.

If the zone changed, SecSpider finds the changed records. Changes can be additions, deletions or modifications to data records or to the DNSKEY records used to sign the data, or simply updates to signatures over existing data. A number of DNSSEC checks are performed too make sure the data is correctly signed, the proper chain of NSEC records are present to prove non-existence of records and so forth.

An overview of this process is shown in the diagram below:



One of the most interesting aspects of this system is the analysis and monitoring of ***vulnerable records***. For any changed data, old versions of the data may present due to existence at valid caches, replay by attackers, or failure to properly remove data due to cache errors. In any case, obsolete DNS data may exist and it may be possible to authenticate this obsolete data via a valid DNSSEC chain. SecSpider tracks and reports via the web any data that was removed from the authoritative server, but may be replayed by an attacker such that this replay will pass the DNSSEC authentication checks.

Based on user feedback, we continue to make small improvements to the tracking and interface for this data. Our software continues to log the data and provides a potentially rich archive on how DNSSEC is being deployed.

4. Task 4: Level 3 Monitoring

Level 3 monitoring is focused on the DNSSEC coordination between zones. To successful deploy DNSSEC, a zone must coordinate with its parent and store a DS record at the parent that corresponds to a DNSKEY record at the zone itself. The coordination of DS record at the parent and DNSKEY at the zone is similar in spirit to the coordination between NS (name server) records that are also stored at both the parent and child. In the SecSpider database, we added monitoring and verification for DNSSEC authentication between zones.

We completed the inclusion of the DS RRs in the monitoring and verification system. The SecSpider tools now monitors the parent zone for each DNSSEC deployed zone. The monitoring system tracks whether the secure has a secure parent. Using a 6 hour poll interval, we can detect whenever a zone's parent deploys DNSSEC and/or creates an authentication chain with its child. The monitor determines whether the delegation is valid and correctly implemented and reports any errors via the SecSpider webpage.

This quarter focused on a final piece of this puzzle; assembling zones into islands of security and tracking how the islands of security evolve. Identifying islands has two components. First, we try to expand the island by moving up the DNS tree. Each secure zone has exactly one parent and often the parent can be found by simply removing the last "." separated field from the name. For example, the parent of "somezone.somewhere.tld." is likely to be "somewhere.tld". Even if this simple check fails to find the parent, it is relatively easy and predictable to move up the tree and find the parent. Once the parent is found, we check whether the parent has configured a DS RR for the secure zone.

The more complex problem arises from finding the child zones below a secure zone. While there is a single parent above the zone, there may be any number of children below the zone. For example, "somezone.somewhere.tld" may have child zones of "otherzone.somewhere.tld", "yetanotherchild.somezone.somewhere.tld", and twohop.childzone.somezone.somewhere.tld". Finding all the child zones is a more challenging and resource intensive task. Our current tool exploits the NSEC records used by secure zones to essentially use the NSEC records to "walk the DNS zone" and identify islands of security. Zone walking raises some privacy issues and the zone walking data is not directly available. We do not believe listing the child zones of a zone raises any concerns and child zones are posted on the website. All data is available on the SecSpider website. With this last piece in place, we believe the base monitoring system is complete. The best source for a complete summary of the monitoring data is the website itself.

5. Task 5: Analysis and Reporting

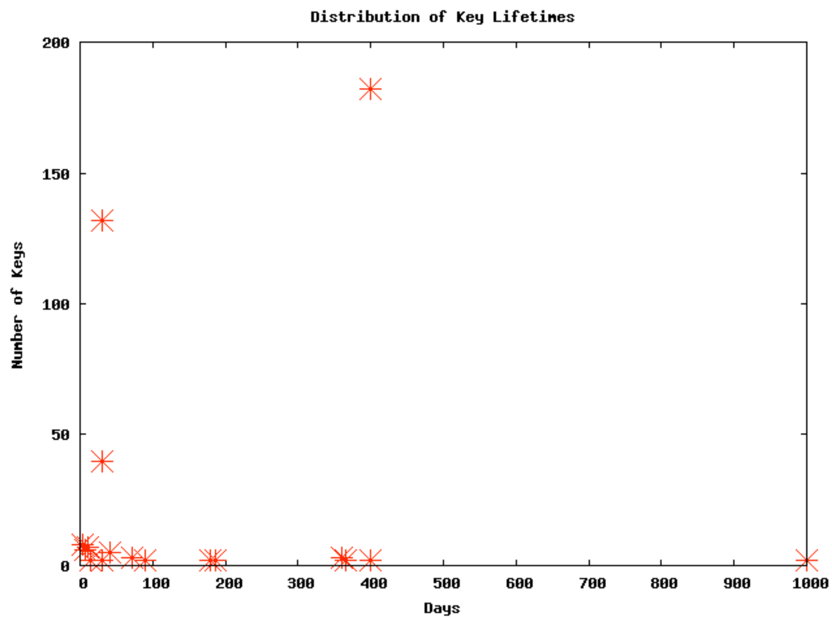
Our initial SecSpider webpage was announced and we received a great deal of feedback which was being incorporated into the new version. Various minor issues range from using UTC time rather than local time (an obvious bug we should have caught) to more complex questions about what it means for an RRSet to vulnerable to replay. The general conclusion was our software was correct, but some softening of the language used was requested. The resulting idea is that the website now conveys an RRSet is vulnerable to attack, but cannot be misunderstood to appear as if an attack has occurred.

Our reports with some zone operators did identify problems with their zones and led to some corrections in their operations. For example, the operators of one zone discovered reachability problems for one of their secondary servers using the monitoring tool. Overall, the tool is providing interesting statistics and our focus is now shifting toward analyzing the resulting monitored data. At a high level, there is one disappointing feature of a small number of secure zones.

Our primary objective was to monitor the deployment of DNSSEC and some more substantial data is now available via the project site. First, the monitor is tracking nearly 2000 zones that are believed to have some relationship to DNSSEC. A zone can be added to this list in four different ways. First, a user may directly submit the zone to the website via a simple interface. For example, a zone administrator that is planning to deploy (or has deployed) DNSSEC may submit their zone. Other users may submit zones that hope will one day deploy DNSSEC. Ideally we would like to monitor every secure zone so we allow anyone to submit a zone. Furthermore, monitoring not yet secure zones is fairly simple and requires little resources from our server so we also allow users to submit any zone they hope may someday deploy DNSSEC. Clearly not all secure zones will submit their name for monitoring. Fundamentally, SecSpider crawls the DNS and looks for new secure zones. We have discovered the vast majority of our zones through the crawling process. Once a secure zone has been found, we add its parent and any children. At this stage, we allow anyone to submit a zone for monitoring

Of the nearly 2000 closely monitored zones, 895 have deployed DNSSEC. Note the other closely monitored not yet secure zones are due to 1) users requesting monitoring for not yet secure zones (a small fraction) and 2) the fact that the parent of a secure zone is automatically added to the monitor list. As discussed later, nearly every secure zone has a not yet secure parent. The number of monitored parents is not equal to 270 since a very small number of zones have secure parents and thus their parent is counted as part of the 270 and many zones share a common parent (e.g. many zones all have "com" as a parent).

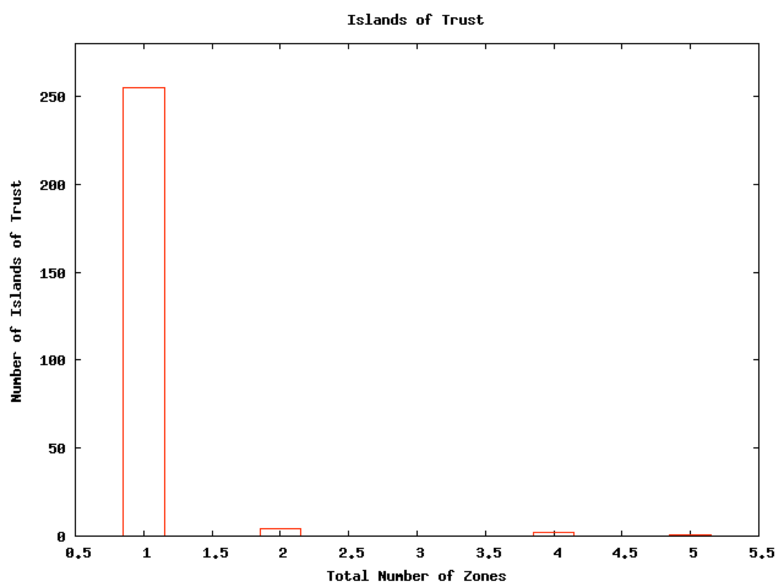
For the secure zones, we track operational practices such as the choice of signature lifetimes. We track 447 DNSKEY records and all but 2 are RSA/SHA1 keys. The signatures over these keys range between 3 and 1,000 days. 80.04% keys signed for either 30 or 400 days. The figure below shows a distribution of key lifetimes and it should also be noted that figure is updated in real-time on the SecSpider website



DNS depends on a tree hierarchy where a parent zone indicates how to reach the name servers for a child zone. DNSSEC extends this coordination so that the parent node also provides a DS record that can be used to authenticate the child's DNSKEY (its public key). The name servers listed at the parent should match the name servers actually used by the child, but a survey earlier in the project showed only 269 (out of 470) authoritative zones have NS RRsets that match the set served by their parents. This is a large concern since DNS can operate even with some errors between the NS records at the parent and child,, but DNSSEC can not tolerate any difference between the DS RR at the parent and the DNSKEY RR at the child. Nearly half of our monitored zones will need to improve their coordination with their parent when DNSSEC is fully deployed.

It is disappointing to see that very few zones arrange DNSSEC coordination with their parent. Fewer than 30 zones (out of 895 DNSSEC deployed) have any DNSSEC coordination between parent and child at the time the project concluded. The largest islands of security at the time are "se." ,"bg.", and "br." and they contain 69, 37, and 29 zones respectively. In our opinion, there is not enough operational experience with DNSSEC coordination between zones and this could be a barrier to large scale deployment.

The figure on the following page shows the size of each island of security. Note that nearly every island of security consists of a single zone that has no authentication leading from the parent zone and no authentication chain leading to any secure children. This is not only an operational concern, it is also a challenge for end resolver. To make full use of DNSSEC, a resolver needs to know the DNSKEY for each island of security. Currently this requires configuring 262 distinct keys into the resovler and updating the list every time a key changes. We believe SecSpider can be used to reduce this burden and have proposed an extension to pursue this direction. Note that as with all graphs, a real-time version of the graph below can be found at on the SecSpider website.



This data provides an interesting first look at DNSSEC deployment.

Our efforts continue on the long TTL discussed in the previous approach and an extensive redesign of the main website was also completed.

6. Summary of Findings

At the conclusion of the project, we believe several major successes were achieved. First, the SecSpider website provides a useful tracking system for monitoring DNSSEC deployment. This site continues to operate and continues to receive feedback. We plan to maintain the website indefinitely, as resources permit.

Based on data from the website and past guidelines by both our team and other groups, DNSSEC deployment guidelines are working reasonably well. Zones are successfully deploying DNSSEC and operations within a single zone seem relatively well managed. SecSpider continues to identify individual zone issues. In particular, SecSpider provides a new DNSSEC administrator with a view of how the outside world sees their deployment. This has allowed operators to catch some errors and provides one with a global view of DNSSEC. In general, we believe deployment within a zone is a success. We are also very excited that a DNSSEC vendor, Secure64, has generally adopted all of our recommendations. This product is in-use at our local sites and currently being marketed.

Based on the data collected, we believe three main challenges remain for the operational community.

1) ***Tool designers must pay very careful attention to default values.*** Our results show that the vast majority of DNSSEC zones operate using lifetimes that match the default values of common tools. It appears very few operators deviate from the default settings and thus choosing appropriate default settings is essential as deployment proceeds.

2) ***More automation would benefit many operations.*** SecSpider tracks when data changes faster than signatures. If a data record changes, an attacker can replay the old record and old signature until the signature expires. By choosing a very long lifetime, one simplifies operations but allows an attacker to replay stale data for a longer time period. SecSpider shows a large number of these stale records. Shortening key and signature lifetimes would reduce the vulnerability, but requires more operational steps. If these steps can be automated, that would be ideal. However automation usually requires an online private key. We strongly recommend online private keys in very secure platforms such as highly protected servers boxes or specialized secure platforms such as those now being sold by Secure64.

3) ***Longer TTL values on infrastructure records are suggested to reduce DDoS vulnerabilities***. DNS relies heavily on caching. Caching individual data records for long times is not recommended since the data may change, but infrastructure records change rarely and tolerate some degree of stale data. Based on data from SecSpider and other monitoring sources, we recommend setting a TTL value of 2 weeks for any infrastructure record (NS record, A record associated with an NS, AAAA record associated with an NS, and DNSKEY record). Our data shows this would dramatically reduce DDoS vulnerabilities. An IETF draft recommending this as a best practice is in progress at the conclusion of this project.

4) ***More need for documentation and automation of inter-zone issues.*** Our final and most important recommendation involves coordination between zones. Without DNSSEC, a zone and its parent (eg. Colostate.edu and edu), must coordinate to ensure a consistent view of the zones nameservers (NS records). Our past studies show this coordination is often plagued by errors that reduce the overall resilience of the system. The nameserver information at the parent only partly matches the actual nameserver data, resulting in a system that still works but is vulnerable to failures if a small number of servers fail. We had hoped DNNSSEC zones would be better at coordination, but the SecSpider data shows this is not the case. As cryptographic proof is added to DNSSEC, it becomes even more essential for zones to have proper information stored at their parent.

What is more troubling is the lack of DNSSEC coordination between zones. Ideally, a zone would have a DS record stored at its parent. The DS record at the parent must match a DNSKEY RR at the zone itself. Unlike the nameserver records which can tolerate some disagreement, this coordination must be exact. A secure zone will be declared invalid if a DS RR at the parent does not match a DNSKEY RR at the child. Very few zones currently coordinate the DNSKEY and DS RR. We believe this is due to the limited deployment of DNSSEC; few parents understand DNSSEC and could support a DS RR. But even when the parent does support DNSSEC, the documentation remains very long and tedious to deploy. We believe parent/child coordination is the main deployment barrier today. Improved documentation and better tools could greatly improve this situation. Automation would be ideal and secure platforms such as the Secure64 product are acting our recommendations. We hope more automated solutions will be available in the future. SecSpider hopes to remain in place and show how this evolves and hopefully also show gains made future improved automation.

7. Project Documents

In addition, our project has produced documents that include the following:

Description	Authors	Venue	Status
The SecSpider Webiste:	Project Team	http://zinc.cs.ucla.edu/secspider	Available
Improving DNS Service Availability by Using Long TTLs	V. Pappas, B. Zhang, E. Osterweil, D. Massey, and L.Zhang	draft-pappas-dnsop-long-ttl	Updated
SecSpider DNSSEC Newsletter Article	Eric Osterweil, Dan Massey, and Lixia Zhang	DNSSEC Newsletter	Published
SecSpider: DNSSEC Monitoring	E. Osterweil, B. Zhang, D.Massey, and L. Zhang	UCLA Engineering Research Symposium	Poster Published
The SecSpider Design	Eric Osterweil, Dan Massey, and Lixia Zhang	DNSSEC Montiroing Project Report	Document Available Online

Guide to Deploying DNSSEC	Kathy Roberston and Dan Massey	Colorado State University Network Security Group Report	Document Published
The DNS Security Extensions	Kathy Roberston and Dan Massey	Colorado State University Undergraduate Research Symposium	Poster Published
Key Management in DNS Security	Bin Zhang and Dan Massey	Colorado State University Computer Science Graduate Research Symposium	Poster Published